DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
3000 MARINE CORPS PENTAGON
WASHINGTON, DC 20350-3000

MCO 5231.3
C4
7 Apr 2009

MARINE CORPS ORDER 5231.3

From: Commandant of the Marine Corps
To: Distribution List

Subj: MARINE CORPS DATA STRATEGY

Ref: (a) DoD Directive 8320.02, "Data Sharing in a Net-Centric
            Department of Defense," December 2, 2004
        (b) DoD Directive 8320.02-G, "Guidance for Implementing Net-Centric
            Data Sharing," April 12, 2006
        (c) DoD Directive 8320.03, "Unique Identification (UID) Standards for
            a Net-Centric Department of Defense," March 23, 2007 (NOTAL)
        (d) Department of Defense Net-Centric Services Strategy, May 04, 2007
        (e) CJCSI 6212.01E, "Interoperability and Supportability of
            Information Technology and National Security Systems,"
            December 15, 2008
        (f) SECNAVINST 5000.36A
        (g) DON CIO Database Registration Memo, March 21, 2008 (NOTAL)
        (h) Net-Centric Data Strategy Working Group (NCDWG) Charter,
            July 19, 2007 (NOTAL)
        (i) DoD Instruction 3020.42, "Defense Continuity Plan Development,"
            February 17, 2006
        (j) DoD and Intelligence Community (IC) Initial Release of Universal
            Core (UCORE) memo of 17 Apr 08
        (k) DoD Discovery Metadata Specification (DDMS), Version 2.0, July 17,
            2008
        (l) SECNAV M-5210.1
        (m) DoD Instruction 8510.01, "DoD Information Assurance Certification
            and Accreditation Process (DIACAP)," November 28, 2007
        (n) DoD Instruction 8500.2, "Information Assurance (IA)
            Implementation," February 6, 2003

Encl: (1) Abbreviations
        (2) Terminology

1. <u>Situation</u>. To provide policy and procedural guidance for the Marine Corps
implementation of the Department of Defense (DoD) Net-Centric Data Strategy
(NCDS) using the Department of the Navy (DON) Functional Data Management (FDM)
construct in accordance with references (a) through (n). The NCDS promotes
the use of data as a shared resource, promotes the independence of data and
data/information exchange from applications/systems, and establishes net-
centricity as a requirement. The DON promotes efficient, effective, and
economical management of data throughout its life cycle.

2. <u>Cancellation</u>. MARADMIN 474/08, MARADMIN 044/08, MARADMIN 415/07, MARADMIN
471/06, and MARADMIN 187/03.

3. <u>Mission</u>. This Order promulgates policy for data production, data storage
and data replication, data/information exchange, participation in NCDS
Communities of Interest (COIs), registration of Authoritative Data Sources
(ADS), and database registration. It also provides Marine Corps personnel a
line of communication to the DON Deputy Chief Information Officer-Marine Corps
(DDCIO-MC) via NCDS tools and the Marine Corps Net-Centric Data Strategy
Working Group (NCDWG).

DISTRIBUTION STATEMENT A: Approved for public release; distribution is
unlimited.

4. Execution

    a. Commander's Intent and Concept of Operations

        (1) Commander's Intent

            (a) To improve critical functions, such as command and control, improve operational effectiveness, and reduce total life cycle management costs, the Marine Corps must improve its ability to share information across functional areas within the Marine Air-Ground Task Force (MAGTF) and with other DoD Combatant Commands/Services/Agencies, federal agencies, state and local governments, tribal governments, non-government organizations, and coalition partners.

            (b) The need to share information must be balanced with our responsibility to protect the information with which we are entrusted. The Marine Corps must conduct information sharing in accordance with applicable laws and regulations, records management policies and Information Assurance (IA) policies.

            (c) The Marine Corps shall embrace net-centric principles where they do not adversely impact or endanger Marines directly engaged in or directly supporting a tactical mission (e.g., armed conflict, disaster relief).

            (d) Marine Corps personnel shall use, update, distribute, and replicate structured (e.g., databases, directories) and unstructured data (e.g., imagery, audio) in accordance with the guidance established in this Order.

            (e) The Marine Corps will use metrics to monitor progress toward implementing the DoD NCDS. These metrics will evolve as doctrine changes and new capabilities are added.

        (2) Concept of Operations

            (a) NCDWG

                1. The Marine Corps NCDWG was chartered in July 2007 to lead the coordinated implementation of the DoD NCDS, and to ensure the data architecture requirements of all Deputy Commandants, Advocates, Proponents, and Marine Corps operating forces are addressed and aligned with the NCDS approach and plan, per reference (h). It is co-chaired by representatives of Headquarters Marine Corps (HQMC) Command, Control, Communications, and Computers (C4); Marine Corps Combat Development Command (MCCDC); and Marine Corps Systems Command (MARCORSYSCOM).

                2. The NCDWG shall review NCDS implementation waivers granted by Functional Area Managers (FAMs)/Functional Data Managers (FDMs) bi-annually to identify issues that need to be addressed by training, policy or governance.

                3. HQMC C4 shall negotiate a standard Service Level Agreement (SLA) with the Defense Information Services Agency (DISA) for each Net-Centric Enterprise Service (NCES) required by the Marine Corps. The NCDWG will adjudicate SLAs for services that are required to implement the DoD Net-Centric Data Strategy (e.g., DoD Metadata Registry (DoD MDR)).

                4. Links to NCDS policies and tools are maintained at the HQMC C4 homepage.

                5. HQMC C4 shall notify Marine Corps personnel via a Marine Corps Bulletin when higher level policy impacting this Order is established or revised. This Order will be updated as needed to incorporate changes to higher level policy and Marine Corps policy.

 6. Contact HQMC C4 for any clarifications or questions regarding this Order.

    (b) NCDS Metrics

 1. The long term objective of collecting and analyzing metrics is to assess the operational and financial benefits associated with implementing standards, eliminating redundancy, and migrating to shared infrastructure.

 2. The initial set of NCDS metrics are simple metrics that are manually collected from NCDS data sources on a quarterly basis. These metrics will be automated as the supporting systems become net-centric, the supporting processes improve, and DoD implements a standard structure for storing and locating data assets in the NCES and DON registries. The NCDS metrics will evolve as the DoD enterprise progresses toward net-centricity.

    (c) Data Production, Storage, and Replication

 1. Marine Corps commands and organizations must reduce redundant manual entry of data. Re-keying data reduces data quality and significantly increases costs when data quality, data reconciliation, and data storage are considered. Marine Corps personnel shall report situations where they manually enter the same data multiple times, via the NCDS tools web page or the FAM/FDM.

 2. Data producers shall tag structured and unstructured data with metadata in accordance with references (a), (b), (e), (k), and this Order.

 3. Data Provenance

 a. Data producers shall tag structured and unstructured data with the date/time that the data originated, unless constrained by tactical reasons.

 b. Data producers shall tag data with origin of production (e.g., person, sensor or chip that originally produced the data) to the maximum extent possible.

 c. These data provenance tags shall be included in all data/information exchanges and downstream repositories.

 d. The date/time and origin associated with all data movement shall be tracked to the maximum extent possible.

 4. Data producers shall ensure the quality, pedigree, security, and accessibility of structured and unstructured data.

 5. The Marine Corps is using a spiral approach to identify and register ADSs. The ADS Directory can be accessed directly, via the NCDS tools web page, or by contacting the FAM/FDM. ADS information will be used to drive data quality improvements and improve resource utilization.

 6. COIs, Programs of Record (PORs), and other initiatives shall use the ADS specified in the ADS Directory rather than launching independent efforts to identify ADSs. Marine Corps personnel shall request changes to the ADS Directory via the NCDS tools web page or FAM/FDM. The ADS Directory and FAM/FDM points of contact are posted on the NCDS tools web page.

 7. If an ADS has been approved for a data/information object, the ADS is the only source that can publish that data on the Global Information Grid (GIG) or distribute that data.

8. Before publishing data on the GIG, the ADS owner shall make their IA policy visible, accessible, and understandable in accordance with references (a), (b), (e), and this Order.

9. Data producers and consumers shall adhere to the IA policies for all data they produce, process, store, receive, or replicate.

10. Consumers of Marine Corps data shall use data from the specified ADS and leverage the standard data distribution service provided by the ADS, rather than requesting custom point to point interfaces.

11. If the ADS is a distributed database, as defined in enclosure (2), the data consumer shall use the data repository at the appropriate echelon.

12. If an ADS is certified as a reporting ADS, the data producer is responsible for ensuring that the data in the reporting ADS is consistent with the data in the ADS. A formal agreement between the ADS and the reporting ADS should be established to ensure data consistency.

13. Data repositories will not be copied to alternate locations unless required to support forward deployed disconnected users; establish a development, testing, or training environment; support fault tolerance and disaster recovery; or support server migration. In the case of forward deployed disconnected users, a sub-set of data relevant to the current mission shall be used when it is sufficient to support warfighter requirements.

14. Requests to replicate data to support reporting requirements shall be submitted to the FAM or FDM.

(d) Data/Information Exchange

1. The Marine Corps endorses the use of net-centric data/information exchanges, such as web services and data published on an Enterprise Service Bus (ESB). Marine Corps organizations exchanging information with other organizations, DoD components, or governmental agencies shall employ net-centric data/information exchanges where they comply with functional and performance requirements. Extensible Markup Language (XML), or a variant thereof, shall be used when there is sufficient bandwidth to support performance requirements.

2. There are circumstances when our forces will be widely dispersed and dependent upon narrowband communications (High Frequency (HF)/Very High Frequency (VHF)/Ultra High Frequency (UHF) Satellite Communications (SATCOM)) as their only means to exchange data/information. When transmitting structured and unstructured data in the tactical domain, the severe limitations imposed by the environment make transmission efficiency a primary concern. Every effort should be made to reduce tactical messages to the smallest size possible. For this reason, the use of tactical message standards and combat net radio protocols are most appropriate. When transmitting imagery, filters should be used to reduce the number of bits transmitted.

3. Units that straddle both the narrowband and broadband environments will need to translate message standards established for each environment. For example, Variable Message Format (VMF) messages may need to be translated to Universal Core standards. Data must be able to be moved bi-directionally between narrowband and broadband environments.

4. MARCORSYSCOM will provide an open, extensible, and modular framework and Service Oriented Environment (SOE) that provides Command Posts with the capability to process, mediate, and exchange message formats from native tactical messages into DoD adopted data standards.

5. All entities that create or update a data/information exchange shall publish associated metadata in the DoD MDR and Service Registry in accordance with references (a), (b), (e), and this Order. The DoD namespace taxonomy will be used once it is established. In the interim, the namespace and/or taxonomy mandated by the Joint Capability Area (JCA) will be used. If a JCA mandate does not exist, the one mandated by the DON will be used. If an applicable JCA or DON mandate does not exist, the namespace and taxonomy specified by the COI or POR will be used.

6. Consumers of data/information exchanges shall adhere to the IA policies and Records Management policies associated with all data they receive, process, or store.

7. Marine Corps personnel are strongly encouraged to use the following information exchange standards where appropriate.

a. Universal Core (UCORE) is an interagency information exchange specification and implementation profile. It provides a framework for sharing the most commonly used data concepts of who, what, when, and where. It serves as a starting point for data level integration and permits the development of richer domain specific exchanges. It was created and is managed by the DoD, Department of Justice (DOJ), Department of Homeland Security (DHS) and Intelligence Community (IC).

b. Command and Control (C2) Core is the family of artifacts consisting of a Joint C2 Conceptual Model and Vocabulary, C2-specific Extensions from the UCORE, the C2 Information Sharing Framework (operational C2 data infrastructure available at the run-time level), and C2 Core Service Specifications.

c. The Joint Consultation, Command and Control Information Exchange Data Model (JC3IEDM) is a logical data that facilitates exchanging data with North American Treaty Organization (NATO) coalition partners.

8. If a program cannot provide a data/information exchange that is compliant with this Order, the Program Manager/Product Group Director shall submit an exception request to the appropriate FAM/FDM.

(e) Communities of Interest (COI)

1. A COI is a collaborative group of users that must exchange information in pursuit of its shared goals, interests, missions, or business processes and, therefore, must have shared vocabulary for the information it exchanges.

2. DoD and non-DoD agencies seeking Marine Corps participation in COIs should contact HQMC C4. HQMC C4 will work with the NCDWG to identify the appropriate FAM/FDM and COI representative(s).

3. All Marine Corps personnel participating in a COI shall register their participation at the Marine Corps COI participation web page or through the appropriate FAM/FDM. When Marine Corps personnel stop participating in a COI, they shall update the appropriate FAM/FDM and COI participation web page.

4. Marine Corps personnel participating in COIs are responsible for ensuring the COI uses the appropriate ADSs, as specified in the Marine Corps ADS Directory.

5. Marine Corps personnel participating in COIs shall ensure the COI publishes metadata in accordance with references (a), (b), (e), and this Order.

6. Marine Corps COI representatives are responsible for identifying and documenting associated costs and benefits associated with COI participation.

(f) <u>Functional Area Management (FAM)</u>

<u>1</u>.   The DON functional area construct is being used for the Marine Corps implementation of the DoD NCDS. Marine Corps FAMs are responsible for ensuring FDM responsibilities are performed in accordance with references (f), (g), and this Order.

<u>2</u>.   FDMs shall work with HQMC elements, MCCDC, MARCORSYSCOM, Program Executive Offices (PEOs) and COIs to do the following within the FAM/FDM portfolio.

<u>a</u>.   Identify ADSs, eliminate redundant data entry and automate data exchange.

<u>b</u>.   Ensure ADSs are registered in the ADS Directory.

<u>c</u>.   Ensure metadata is registered in the DoD MDR, NCES Services Registry and Enterprise Catalog.

<u>d</u>.   Identify and eliminate unnecessary redundant data repositories.

<u>e</u>.   Assist in the coordination of JCA common core development.

<u>f</u>.   Approve/disapprove data exchange waivers.

<u>g</u>.   Approve/disapprove requests to replicate data to support reporting requirements.

<u>h</u>.   Work with data owners to establish, define, monitor and enforce data quality.

<u>i</u>.   Ensure that records management requirements are built into agency Information Technology (IT) governance processes for capital planning, enterprise architecture, business process, design, and the systems development life cycle.

<u>3</u>.   FDMs shall work with data producers to ensure all databases that are hosted on a server or a mainframe are registered in accordance with reference (g) and this Order.

<u>a</u>.   If a system/application is registered in DoD Information Technology Portfolio Registry – Department of the Navy (DITPR-DON)/DON Applications and Database Management System (DADMS) and it has a database that is used to store Marine Corps data, the database must be registered in DADMS.

<u>b</u>.   If the DADMS record is used to track a Commercial-Off-The-Shelf (COTS) software license rather than a physical implementation, the record should not indicate that there is a database.

<u>c</u>.   Databases created on a laptop/desktop computer for personal use do not need to be registered in DADMS.

<u>d</u>.   The FDM will determine when databases that were not intended to be lasting need to be registered in DADMS.

<u>e</u>.   Nothing should be entered into DADMS that would result in the disclosure of classified information.

<u>f</u>.   Databases created as hot backup sites should be registered in DADMS.

g. Databases shall be registered in DADMS in the following priority: 1) approved ADSs, 2) databases which exchange information with other external databases or systems, and 3) all other databases.

h. Databases and data repositories on sensor platforms and tactical end-item equipment and weapons do not need to be registered in DADMS.

(g) Information Assurance (IA)

1. Information assurance compliance is a critical component of the Marine Corps implementation of the DoD NCDS. As such, all Marine Corps data must be hosted on systems that comply with references (m) and (n).

2. Vital data sources are those structured and unstructured data sources that are needed to support mission essential functions and those sources required to reconstitute normal operations after a crisis. All vital data sources must be made survivable, accessible, and discoverable from alternate locations. Disaster recovery, contingency plans, and business continuity plans are required for vital data sources in accordance with reference (i).

3. Marine Corps personnel shall overwrite and purge Personally Identifiable Information (PII) data/information between war fighting and humanitarian missions. This is particularly important as spillage could result in violating civil rights and legal action.

b. Subordinate Element Missions. The Deputy Commandants for Aviation; Installation and Logistics; Plans, Policies, and Operations; Programs and Resources; and Combat Development and Integration Departments; the Director, C4/DDCIO-MC; Director, Intelligence Department; and Commanding General, Marine Corps Systems Command shall ensure all agencies/entities under their sponsorship or direction comply with the provisions of this Order.

5. Administration and Logistics. Organizations responsible for formulating policy, writing requirements, developing systems/applications, and validating systems performance must do so in accordance with the instructions and policies in this Order.

6. Command and Signal

a. Command. This Order is applicable to the Marine Corps Total Force.

b. Signal. This Order is effective the date signed.

R. S. KRAMLICH
Director, Marine Corps Staff

DISTRIBUTION: PCN 10208711400

ABBREVIATIONS

ADS	Authoritative Data Source
AFATDS	Advanced Field Artillery Tactical Data System
C2	Command and Control
C2ISF	C2 Information Sharing Framework
C4	Command, Control, Communications and Computers
CIO	Chief Information Officer
COI	Community of Interest
COTS	Commercial Off The Shelf
DADMS	DON Application and Database Management System
DDMS	DoD Discovery Metadata Specification
DDCIO-MC	DON Deputy Chief Information Officer - Marine Corps
DHS	Department of Homeland Security
DIACAP	DoD Information Assurance Certification and Accreditation Process
DISA	Defense Information Systems Agency
DITPR-DON	Department of Defense Information Technology Portfolio Repository - Department of the Navy
DOJ	Department of Justice
DoD	Department of Defense
DoD MDR	DoD Metadata Registry
DON	Department of the Navy
ESB	Enterprise Service Bus
EXI	Efficient XML Interchange
FAM	Functional Area Manager
FDM	Functional Data Manager
FSCC	Fire Support Control Center
GIG	Global Information Grid
GML	Geography Markup Language
HF	High Frequency
HQMC	Headquarters Marine Corps
IA	Information Assurance
IC	Intelligence Community
IC ISM	IC Information Security Marking

IT	Information Technology
JC3IEDM	Joint Consultation Command and Control Information Exchange Data Model
JCA	Joint Capability Area
JTCW	Joint Tactical Common Operational Picture Workstation
LDAP	Local Directory Access Protocol
LEXS	Law Enforcement Information Sharing Program Exchange Specifications
MAGTF	Marine Air-Ground Task Force
MARCORSYSCOM	Marine Corps Systems Command
MCCDC	Marine Corps Combat Development Command
MCEN	Marine Corps Enterprise Network
NATO	North American Treaty Organization
NCDS	Net-Centric Data Strategy
NCES	Net-Centric Enterprise Services
NCDWG	Net-Centric Data Strategy Working Group
NGO	Non-Governmental Organization
NIEM	National Information Exchange Model
NOTAL	Not to, nor required by, all addressees
PEO	Program Executive Office(s)
PII	Personally Identifiable Information
POR	Program of Record
RDF	Resource Description Framework
SATCOM	Satellite Communications
SECNAV	Secretary of the Navy
SLA	Service Level Agreement
SOA	Service-Oriented Architecture
SOE	Service Oriented Environment
UCORE	Universal Core
UHF	Ultra High Frequency
UID	Unique Identification
ULEX	Universal Lexical Exchange
USMC	United States Marine Corps
VHF	Very High Frequency

VMF	Variable Message Format
WSDL	Web Services Description Language
XML	Extensible Markup Language
XSD	XML Schema Definition

TERMINOLOGY

1. <u>Application</u>. A software tool that functions and is operated on a computer.

2. <u>Authoritative Data Source (ADS)</u>. A recognized or official data production source with a designated mission statement or source/product to publish reliable and accurate data for subsequent use by customers. An authoritative data source may be the functional combination of multiple, separate data sources.

3. <u>Command and Control (C2)</u>. The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. C2 functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission.

4. <u>Command and Control (C2) Core</u>. The family of artifacts consisting of a Joint C2 Conceptual Model and Vocabulary, C2-specific Extensions from the UCORE, the C2 Information Sharing Framework (operational C2 data infrastructure available at the run-time level), and C2 Core Service Specifications.

    a. <u>Joint C2 Conceptual Model and Vocabulary</u>. A service which publishes descriptions of C2 entities and their interrelationships together with terms and definitions that express properties of those entities.

    b. <u>C2 Specific Extensions from the UCORE</u>. Schema components and vocabulary extended from the UCORE as required, providing an ability to share more detailed data within the C2 community. C2 specific extensions from UCORE would be under configuration management of the C2 Capability Portfolio Manager in cooperation with the C2 community.

    c. <u>C2 Information Sharing Framework (C2ISF)</u>. A run-time infrastructure that enables data sharing necessary for command and control of operations. This infrastructure, which exploits DoD enterprise infrastructure, includes registries (service, metadata), content catalogs, access control arrangements, mediators, crawlers and tagging engines, development and test tool kits, and instrumentation to provide user feedback, metrics collection, and fact checking capabilities.

    d. <u>C2 Core Service Specifications</u>. Specification for cooperating C2 mission services that actually perform functions required to support command and control of operations.

5. <u>Community of Interest (COI)</u>. A collaborative group of users that must exchange information in pursuit of its shared goals, interests, missions, or business processes and therefore must have shared vocabulary for the information it exchanges.

6. <u>Data Consumer</u>. Refers to a program, organization, or person that uses data or data assets (e.g., system developer, ad-hoc report).

7. <u>Data Owner</u>. Refers to the program, organization, or person which determines the purposes and means of the processing of a particular collection of data.

8. <u>Data Producer</u>. Refers to a program, system, sensor (manned or unmanned), organization, or person that controls, manufactures, or maintains data or data assets.

9. <u>Data Repository</u>. A place where structured or unstructured data is stored. This includes structured repositories such as relational databases, object-oriented databases, and Local Directory Access Protocol (LDAP) directories. This also includes unstructured repositories, such as imagery libraries and document repositories.

10. <u>Database</u>. A collection of interrelated data, often with controlled redundancy, organized according to a schema to serve one or more applications; the data is stored so that different programs can use them without concern for the data structure or organization. Databases include relational databases, object-oriented databases, XML databases, etc.

11. <u>Department of Defense Information Technology Portfolio Repository –
Department of the Navy (DITPR-DON)</u>. DITPR-DON is the single, authoritative source for data regarding DON Information Technology (IT) systems, including National Security Systems. Registration of mission-critical, mission-essential, and mission-support systems in DITPR-DON is central to establishing an accurate and reliable enterprise-wide inventory. Additionally, DITPR-DON is used to satisfy statutory and management reporting requirements, including Federal Information Security Management Act reporting and the Business Management Modernization Program certification process.

12. <u>Distributed Database</u>. Distributed databases are required in a tactical environment for security and survivability. They are also required due to limited bandwidth and connectivity. In a distributed database, each node has the entire set of data it requires, and some data is aggregated to higher commands. For security reasons, there is no way to connect to all nodes and aggregate all the data. Tactical systems, such as the Advanced Field Artillery Tactical Data System (AFATDS) and the Joint Tactical Common Operational Picture Workstation (JTCW), employ distributed databases. Each system replicates and synchronizes data with a limited number of nodes in a way that is consistent with the needs of the users. For example, a battalion Fire Support Control Center (FSCC) may backup its data with the regimental FSCC.

13. <u>DoD Metadata Registry (DoD MDR)</u>. As part of the overall DoD NCDS, the DoD CIO established the DoD MDR and a metadata registration process for the collection, storage, and dissemination of structural metadata information resources (schemas, data elements, attributes, document type definitions, style-sheets, data structures, etc.). This web-based repository is designed to also act as a clearinghouse through which industry and government coordination on metadata technology and related metadata issues can be advanced.

14. <u>DON Application and Database Management System (DADMS)</u>. The ADS for DON IT and National Security Systems applications and database inventory registration.

15. <u>Enterprise Service Bus (ESB)</u>. An infrastructure software product that brings flow related concepts such as transformation and routing to a Service-Oriented Architecture (SOA).

16. <u>Extensible Markup Language (XML)</u>. A general-purpose markup language capable of describing many different kinds of data (e.g., Geography Markup Language (GML), Resource Description Framework (RDF), XML Schema Definition (XSD), Web Service Definition Language (WSDL)). The primary purpose is to facilitate the sharing of data across different systems, particularly systems connected via the World Wide Web.

17. <u>Functional Area Manager (FAM)</u>. The individual or designated agency responsible for the management and planning of all personnel and equipment within a specific functional discipline.

18. <u>Functional Data Manager (FDM)</u>. The individual designated by the respective FAM to produce and control structuring of data and metadata within functional activities, information systems, and computing and communications infrastructures.

19. <u>Global Information Grid (GIG)</u>. The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policymakers, and support personnel. The GIG includes

all owned and leased communications and computing systems and services, software (including applications), system data, security services, and other associated services necessary to achieve information superiority for the United States military. It is the physical manifestation of the network-centric warfare doctrine. The Marine Crops Enterprise Network (MCEN) falls under the umbrella of the GIG.

20. <u>Information Assurance (IA)</u>. Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.

21. <u>Information Technology (IT)</u>. Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used directly or is used by a contractor under a contract with the executive agency which requires the use of such equipment; or requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "information technology" also includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. The term "information technology" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.

22. <u>Marine Corps Systems Command (MARCORSYSCOM)</u>. The Commandant's principal agent for acquisition and sustainment of systems and equipment used by the operating forces to accomplish their mission.

23. <u>Net-Centric Enterprise Services (NCES)</u>. The NCES is a Defense Information Services Agency acquisition program to adopt, buy, or create essential information sharing services needed by the DoD. As part of the common infrastructure, it will enable seamless information sharing by providing enterprise-wide services for characterizing, cataloging, locating, and accessing information on the GIG. NCES is the only program specifically tasked with providing enterprise-wide information sharing capabilities to enable information superiority, accelerated decision-making, and effective operations.

24. <u>Net-Centric Data Strategy (NCDS)</u>. The DoD NCDS provides a key enabler of the DoD's transformation by establishing the foundation for managing the DoD's data in a net-centric environment.

25. <u>Net-Centric Data Strategy Working Group (NCDWG)</u>. The Marine Corps NCDWG leads the coordinated implementation of the USMC NCDS.

26. <u>Reporting Authoritative Data Source</u>. A recognized or official data source, that is not the originating ADS, with a designated mission statement or source/product to publish reliable and accurate data for subsequent use by customers. A reporting authoritative data source may be the functional combination of multiple, separate data sources.

27. <u>Service</u>. A combination of people, processes, and technologies provided to one or more customers by an IT service provider.

28. <u>System.</u> A combination of interrelated and interacting hardware, software and firmware that functions as a coherent entity.

29. <u>Taxonomy</u>. A set of controlled vocabulary terms, usually hierarchical.

30. <u>Universal Core (UCORE)</u>. UCORE is an interagency information exchange specification and implementation profile. It provides a framework for sharing the most commonly used data concepts of who, what, when, and where. It serves as a starting point for data level integration and permits the development of

richer domain specific exchanges. It was created and is managed by DoD, Department of Justice (DOJ), Department of Homeland Security (DHS) and the Intelligence Community (IC).

31. <u>Web Service</u>. A standardized way of integrating web-based applications using open standards over an Internet Protocol backbone. Web services allow applications developed in various programming languages and running on various platforms to exchange data without intimate knowledge of each application's underlying IT systems.